UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,073	03/16/2004	Leemon C. Baird III	TRO-0301C	3771

83694 7590 12/24/2008
Fay Kaplun & Marcin, LLP/ Motorola
150 Broadway Suite 702
New York, NY 10038

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/802,073	BAIRD ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *50,51,54-61 and 64-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *50, 51, 54-61, 64-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 27, 2008 has been entered. Claims 50, 60 and 70 have been amended. Claims 52, 53, 62 and 63 have been amended. Claims 50, 51, 54-61,a and 64-70 are pending and have been considered below.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 50, 60 and 70 recite the limitation "the verification" in line 8 and line 7. There is insufficient antecedent basis for this limitation in the claim.

Specification

4. the objection to the specification has been withdrawn.

Claim Rejections - 35 USC § 101

5. the 101 rejection to claim 70 has been withdrawn.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 50, 51, 55, 56, 60, 61, 65, 66 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullman et al (US 5,280,527). In view of Zingher et al (US 5,731,575) in further view of Haverstock et al (US 6,701,376).

Claims 50, 60 and 70: Gullman et al discloses a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, comprising:

i. A memory storing data related to at least one of accounts and preferences (*memory stores a template of authorized user) (column 2, lines 48-55);* and

ii. A processor coupled to the memory(*Fig. 2*), the processor authenticating the user with the device by verifying a device password and a user biometric that are specific to the device *(upon entry of the cardholder's biometric information, the processor executes the verification algorithm) (column 2, lines 53-55*) and transmitting a resource password (t*oken*)to establish a connection to the network resource, the resource password being unknown to the user and specific to the network resource

(*the verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN embedded serial number, account number) and time-varying self-generated information to derive a token output. In an alternative embodiment, the token output is transmitted directly to the host system through a direct data communication line, eliminating the need for manual entry by the user) (column 2, lines 55-65).*

Gullman et al does not explicitly disclose wherein a duress password is entered for the verification, the duress password being predetermined to be used when an access to the device is intended to be denied, or wherein the entry of the duress password replaces the data of the memory with non-sensitive data. However Zingher et al discloses a computerized system and method which further discloses wherein a duress password is entered for the verification, the duress password being predetermined to be used when an access to the device is intended to be denied(*assigning a second PIN or Personal Distress Number or PDA to a cardholder)(column 7, lines 24-35; Fig. 5, 7, 8 item 65*).

While neither of them explicitly wherein the entry of the duress password replaces the data of the memory with non-sensitive data. However, Haverstock et al discloses a web server enabling browser access to HTML and non HTML document which further discloses explicitly wherein the entry of the duress password replaces the data of the memory with non-sensitive data (*column 7, line 30 to column 8, line 58 which specify that when a user request a resource*

access to the resource is based on who the user is, by using the duress password the user will access to the system but with less privilege).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Gullman et al such as to use a duress password and In to modify the combined teaching of Gullman et al and Zingher et al such as replace data with non sensitive data. One would have been motivated to do the above modifications in order to prevent unauthorized transaction as taught by Zingher et al (column 1, lines 5-10) and in order to restrict access to sensitive data based on user role as taught by Haverstock et al (*column 7, lines 20-30*).

Claims 51 and 61: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 50 and 60 above, and Gullman et al further discloses wherein the user is granted access to the memory upon verification (*the access device 12 transmits the token to the host 10 which decrypts or decodes the token to derive the fixed code and correlation factor. If the fixed code identifies a valid user and the correlation factor is above the threshold level, then access is permitted) (column 6, lines 37-45*).

Claim 55 and 65: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 50 and 60 above, and Gullman et al further discloses wherein the user biometric is at least one of a

path and a speed era use of an input device, a fingerprint description, an iris scan, and a voice print (*column 3, lines 55-67; column 5, lines 42-55*).

Claims 56 and 66: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 55 and 65 above, and Gullman et al further discloses wherein the path and the speed of the use of the input device include a signature of the device password to combine the device password and the biometric for the verification(*column 3, lines 55-67; column 5, lines 42-55*).

8. Claims 54, 57-59, 64 and 67-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullman et al (US 5,280,527) in view of Zingher et al (US 5,731,575) and Haverstock et al (US 6,701,376) in further view of Chou et al (US 5,638,444).

Claims 54 and 64: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 50 and 61 above, while neither of them explicitly disclose wherein the data of the memory is encrypted, the data being decrypted with a device dependent key specific to the device. However, Chou et al discloses a secure computer communication method and device, which further discloses wherein the data of the memory is encrypted, the data being decrypted with a device dependent key specific to the device (*column 1, lines 20-65*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of

Gullman et al , Zingher et al and Haverstock et al such as to decrypt the data by using a device dependant key. One would have been motivated to do so in order to provide secure and ciphered communication between any types of computer as taught by Chou et al (*column 1, lines 5-10*).

Claims 57 and 67: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 50 and 60 above, while neither of them explicitly disclose that a true random number generator generating the resource password. However, Chou et al discloses a secure computer communication method and device, which further discloses that a true random number generator generating the resource password (*column 1, lines 34-40; Fig. 2*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Gullman et al , Zingher et al and Haverstock et al such as to use a random number generator to generate the session key. One would have been motivated to do so in order to provide secure and ciphered communication between any types of computer as taught by Chou et al (*column 1, lines 5-10*).

Claims 58 and 68: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 50 and 60 above, while neither of them explicitly disclose wherein the resource password is generated at a predetermined time for the access to the network resource.

However, Chou et al discloses a secure computer communication method and device, which further discloses wherein the resource password is generated at a predetermined time for the access to the network resource (*Fig. 2*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to the combined teaching of Gullman et al , Zingher et al and Haverstock et al such as to generate the resource password at a predetermined time. One would have been motivated to do so in order to provide secure and ciphered communication between any types of computer as taught by Chou et al (column 1, lines 5-10).

Claims 59 and 69: Gullman et al , Zingher et al and Haverstock et al disclose a device for providing a user with a secure access to a network resource and a method for authenticating a user to a device, as in claims 55 and 60 above, while neither of them explicitly discloses wherein communications with the network resource are encrypted. However, Chou et al discloses a secure computer communication method and device, which further discloses wherein communications with the network resource are encrypted (*column 1, lines 20-65).* Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Gullman et al , Zingher et al and Haverstock et al such as to encrypt the communication with the network resource. One would have been motivated to do so in order to provide secure and ciphered communication between any types of computer as taught by Chou et al (column 1, lines 5-10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Ft,

Monday December 22, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436